

8. Символ Лежандра. Свойства. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$. Вычисление $\left(\frac{-1}{p}\right)$.

9. Формула $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$.

+задача

Определение

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}$. Тогда **символ Лежандра**

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ — квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ — квадратичный невычет по модулю } p; \\ 0, & \text{если } a \vdots p. \end{cases}$$

Свойство 1

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Доказательство. • a — квадратичный вычет по модулю p
 $\iff \bar{a}$ — квадратичный вычет в $\mathbb{Z}_p \iff (\bar{a})^{\frac{p-1}{2}} = 1$.

• a — квадратичный невычет по модулю p \iff
 \bar{a} — квадратичный невычет в $\mathbb{Z}_p \iff (\bar{a})^{\frac{p-1}{2}} = -1$.

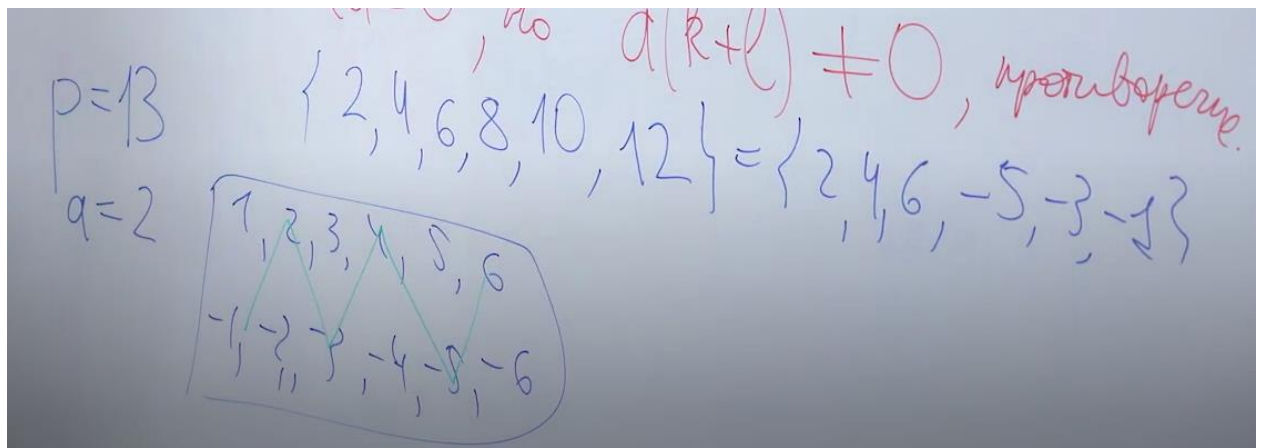
• $a = 0 \iff a^{\frac{p-1}{2}} = 0$. □

Выяснение квадр. хар-ра $\left(\frac{a}{p}\right)$ Лемма Гаусса:

$\left(\frac{a}{p}\right) = 1$, если в списке $\left\{a, 2a, 3a, \dots, \frac{p-1}{2}a\right\}$,
 после приведения его к виду $\{\pm 1, \pm 2, \dots, \pm \frac{p-1}{2}\}$,
 будет чётное число отрицательных; $\left(\frac{a}{p}\right) = -1$, если их нечётно.

От противного: пусть $ka = b$, $la = -b$
 $\Rightarrow ka + la = 0$, но $a(k+l) \neq 0$, противоречие.
 2, 4, 6, 8, 10, 12

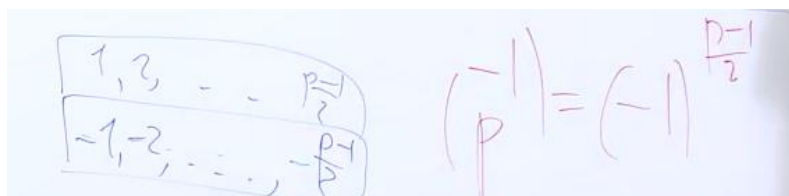
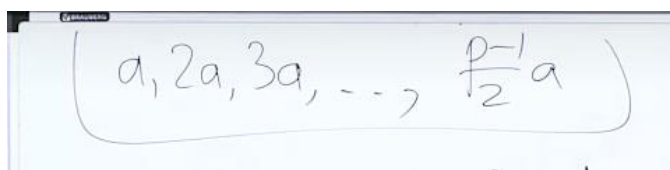
(± 8) $p=13$
 $a=2$



Свойство 2

(Первое дополнение к закону взаимности Гаусса.)

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$



«Молния» проходит только в нижней части «чемодана Гаусса»

Свойство 3

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Доказательство. • Следует из Леммы 5 и определения символа Лежандра.



Лемма 5

Пусть $p \in \mathbb{P}$, $a, b \in \mathbb{Z}_p$, $a \neq 0$, $b \neq 0$. Тогда:

- 1) Если a, b — квадратичные вычеты, то ab — квадратичный вычет.
- 2) Если a — квадратичный вычет, а b — квадратичный невычет, то ab — квадратичный невычет.
- 3) Если a, b — квадратичные невычеты, то ab — квадратичный вычет.

$$1 * 1 = 1;$$

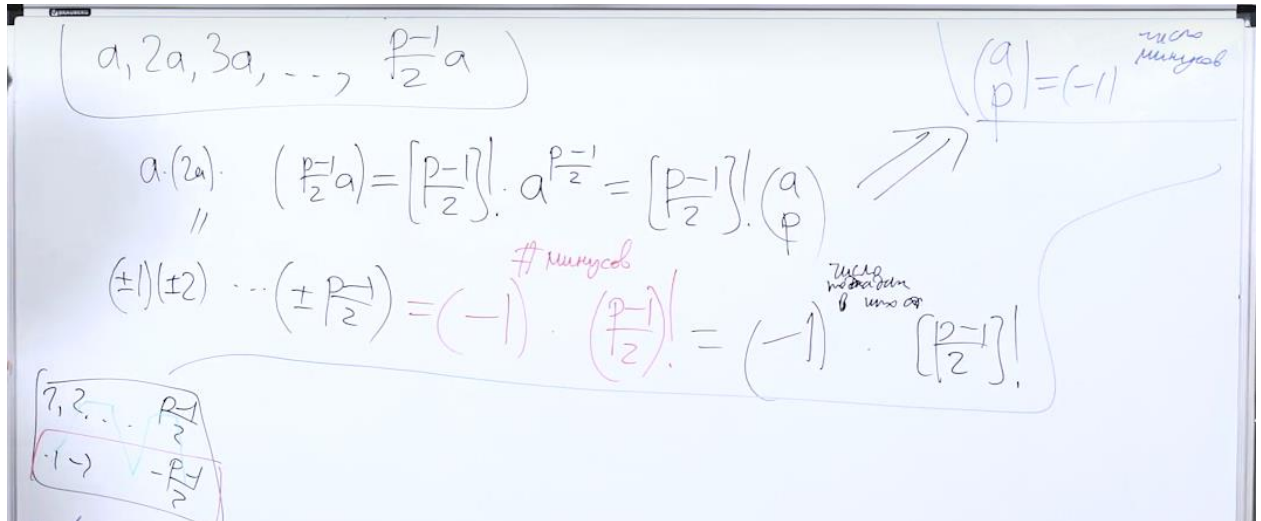
$$1 * (-1) = -1;$$

$$(-1) * (-1) = 1$$

Лемма 6

Пусть $p \in \mathbb{P}$, $p_1 = \frac{p-1}{2}$, $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{p}$. Тогда

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{2ax}{p}\right]}.$$



$$a = 2; p = 29$$

2; 2*2; 3*2; 4*2; 5*2; 6*2; 7*2; 8*2; 9*2; 10*2; 11*2; 12*2; 13*2; 14*2

2	4	6	8	10	12	14	16	18	20	22	24	26	28
2	4	6	8	10	12	14	-13	-11	-9	-7	-5	-3	-1

1	2	3	4	5	6	7	8	9	10	11	12	13	14
-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	-11	-12	-13	-14

Доказательство. • Пусть $M = \{1, 2, \dots, p_1\}$.

Утверждение 1

Для каждого $j \in M$ существует $s_j \in \{0, 1\}$ и $r_j \in M$ такие, что $ja \equiv (-1)^{s_j} r_j \pmod{p}$.

Доказательство. • Пусть r'_j — остаток от деления ja на p .

- Если $r'_j \in M$, то положим $r_j := r'_j$, $s_j = 0$.
- Если $r'_j \notin M$, то $r'_j \in \{p_1 + 1, \dots, p - 1\}$, тогда $p - r'_j \in \{1, \dots, p - 1 - p_1 = p_1\} = M$.
- В этом случае положим $r_j = p - r'_j$, $s_j = 1$. □

Утверждение 2

Если $i, j \in M$, $i \neq j$, то $r_i \neq r_j$.

Доказательство. • Предположим противное, пусть $r_i = r_j$.

- Если $s_i = s_j$, то $r'_i = r'_j$.
- Следовательно, $ia \equiv_p ja \iff a(i-j) \vdots p \Rightarrow i-j \vdots p$, что не так (последний переход верен, так как $(a, p) = 1$).
- Если $s_i \neq s_j$, то $r'_i = p - r'_j$.
- Следовательно, $ia \equiv_p -ja \iff a(i+j) \vdots p \Rightarrow i+j \vdots p$, что не так: $2 \leq i+j \leq 2p_1 = p-1$. □

Утверждение 3

$$s_j = 1 \iff \left[\frac{2aj}{p} \right] \not\equiv 2.$$

Доказательство. • Напомним, что

$$aj = pq + r'_j \iff 2aj = 2pq + 2r'_j, \text{ где } r'_j \in \{1, \dots, p-1\}.$$

$$\begin{aligned} s_j = 1 &\iff \frac{p+1}{2} = p_1 + 1 \leq r'_j \leq p-1 \iff \\ p+1 &\leq 2r'_j \leq 2p-2 \iff p+1+2pq \leq 2aj \leq 2p-2+2pq \iff \\ p+2pq &< 2aj < 2p+2pq \iff \\ 2q+1 &< \frac{2aj}{p} < 2q+2 \iff \left[\frac{2aj}{p} \right] = 2q+1 \not\equiv 2. \end{aligned}$$

- **Пояснение 1.** Так как разность целых чисел не менее 1, $p+1+2pq \leq 2aj \iff p+2pq < 2aj$.
- **Пояснение 2.** Так как разность четных чисел не менее 2, $2aj \leq 2p-2+2pq \iff 2aj < 2p+2pq$. □

- Вернемся к доказательству Леммы 6. По Утверждению 2, $\{r_1, \dots, r_{p_1}\} = M$ (так как все эти числа из M и различны, а $|M| = p_1$).
- Пусть $R = 1 \cdot 2 \cdot \dots \cdot p_1$. Тогда $r_1 r_2 \cdot \dots \cdot r_{p_1} = R$.
- Напишем цепочку сравнений:

$$(-1)^{\sum_{x=1}^{p_1} s_x} R \equiv (-1)^{\sum_{x=1}^{p_1} s_x} \cdot \prod_{x=1}^{p_1} r_x \equiv$$

$$\prod_{x=1}^{p_1} (-1)^{s_x} r_x \equiv \prod_{x=1}^{p_1} ax \pmod{p} \equiv a^{p_1} R \pmod{p} \quad (1).$$

- Сокращая (1) на R (можно, так как $(R, p) = 1$),

получаем $a^{p_1} \equiv (-1)^{\sum_{x=1}^{p_1} s_x} \equiv (-1)^{\sum_{x=1}^{p_1} [\frac{2ax}{p}]} \pmod{p}$
 (последний переход верен по Утверждению 3). □

Лемма 6

Пусть $p \in \mathbb{P}$, $p_1 = \frac{p-1}{2}$, $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{p}$. Тогда

$$p_1 = \frac{p-1}{2}$$

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} [\frac{2ax}{p}]}.$$

Handwritten notes on a chalkboard showing the proof of Lemma 6. The notes include the definition of $p_1 = \frac{p-1}{2}$, the product of residues r_1, \dots, r_{p_1} , and the derivation of the Legendre symbol formula using properties of quadratic residues and the law of quadratic reciprocity.

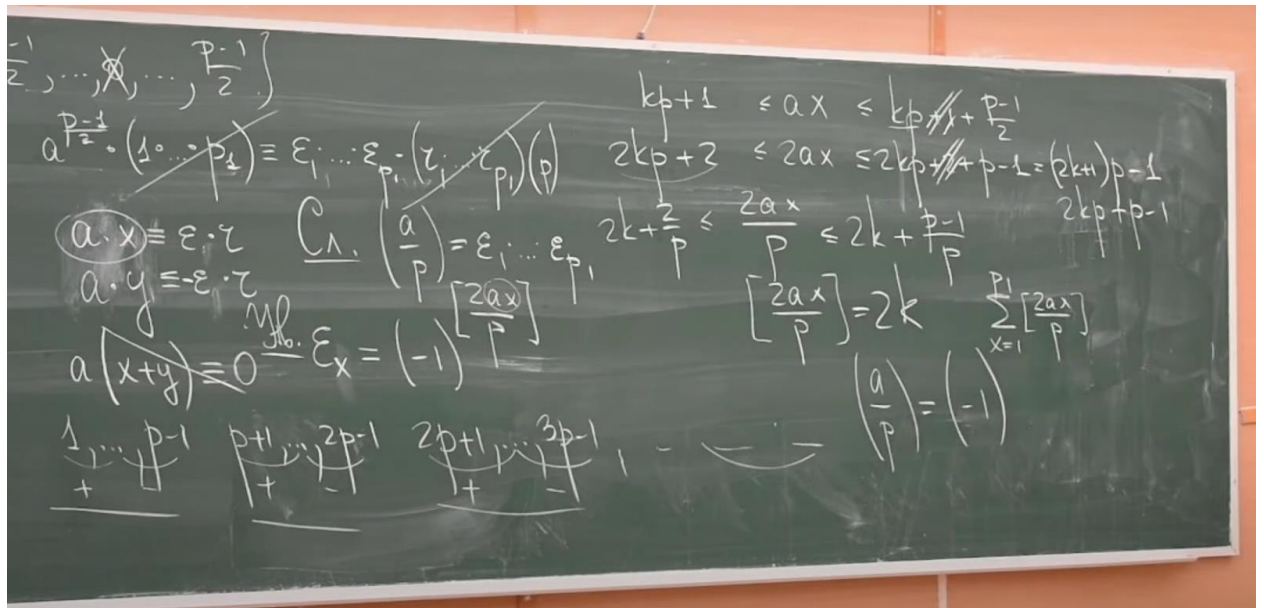
Top line: $\left[-\frac{p-1}{2}, \dots, \cancel{0}, \dots, \frac{p-1}{2}\right]$

Left side:

- $a \cdot 1 \equiv \varepsilon_1 \cdot \zeta_1 \pmod{p}$
- $a \cdot p_1 \equiv \varepsilon_{p_1} \cdot \zeta_{p_1} \pmod{p}$
- $\varepsilon_i = \pm 1$
- $\zeta_i \in \{1, \dots, p_1\}$

Right side:

- $a^{\frac{p-1}{2}} \cdot (1 \cdot \dots \cdot p_1) \equiv \varepsilon_1 \cdot \dots \cdot \varepsilon_{p_1} \cdot (\zeta_1 \cdot \dots \cdot \zeta_{p_1}) \pmod{p}$
- $a \cdot x \equiv \varepsilon \cdot \zeta$
- $a \cdot y \equiv -\varepsilon \cdot \zeta$
- $a(x+y) \equiv 0 \pmod{p}$
- $\varepsilon_x = (-1)^{[\frac{2ax}{p}]}$
- $\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \dots \cdot \varepsilon_{p_1}$



Теперь оценим аналогично, если ax попадает в «правую» половину

$$\frac{p-1}{2} + 1 + kp \leq ax \leq kp - 1 + p$$

$$p - 1 + 2 + 2kp \leq 2ax \leq 2kp - 2 + 2p$$

$$p(2k+1) + 1 \leq 2ax \leq 2kp - 2 + 2p$$

$$(2k+1) + \frac{1}{p} \leq \frac{2ax}{p} \leq 2k + 2 - \frac{2}{p}, \text{ то есть}$$

$$\left\lfloor \frac{2ax}{p} \right\rfloor = 2k + 1, \text{ в общем, нечётное число.}$$

Задача:

Сколько корней имеет

$$x^4 + 20 = 0 \text{ в } F_{101}?$$

$$x^4 = 81 \text{ в } F_{101}$$

$(x^2 - 9)(x^2 + 9) = 0$ (то есть надо посмотреть, является ли 9 и -9 квадратичным вычетом по модулю 101)

$$\left(\frac{9}{101}\right) = \left(\frac{3}{101}\right)^2 = 1, \text{ то есть } 9 - \text{квадратичный вычет по модулю } 101$$

$$\left(\frac{-9}{101}\right) = \left(\frac{-1}{101}\right) \left(\frac{9}{101}\right) = (-1)^{\frac{101-1}{2}} * 1 = 1, \text{ то есть } -9 - \text{квадратичный вычет по модулю } 101$$

